Result Page

The present invention refers to a membrane anti elastomer

intrusion for protected electronic packages. It applique with the made safe housings, such as particularly the housings confidential codes, which one seeks to guarantee the physical integrity by a mean of detection of opening. The protected electronic packages are used in numerous applications and particularly make it possible to read chip cards such as for example bank cards, porte-monnaie

▲ top electronic, of the cards multiservices (telephonic, banking, carries

electronic money, health...) or of the privative charge cards.

In order to avoid the frauds, they are equipped with systems protections, such as

devices anti-intrusion, which guarantee their physical integrity.

One can quote the example of the terminals of electronic payment (TPE), particularly by bank card. These electronic terminals are the target of swindlers who try by all the means to open them and to modify them for a fraudulent use. In reaction, the organisms of bank card, such as Aimed International, force constraining norms of safety to approve these terminals of payment. According to one of these norms, the terminals must be in measurement to detect any attempt at opening of their housing. The detection of the opening involves particularly the disablement of the safety module, which contains for example a whole of cryptographic algorithms and codes secret being used to validate the chip card or card with magnetic track and to ensure the integrity of

information of payment (meters of units or transactions).

The terminals of electronic payment by bank card comprise sometimes houslngs confidential codes, still called Pinpad in the Anglo-Saxon literature. These housings are used for reading a bank card, entering its secret code, and checking the validity of the entered code. They comprise generally a digital keyboard, a screen with liquid crystals, a reader of chip card, optionally a cache codes, and a connection by wire to a point-of-sale terminal. In this example, the terminal of electronic payment is the unit made up of the housing codes confidential and

point-of-sale terminal.

In the technical current ones, the terminals of electronic payment are equipped with switches which detect the opening. These switches are placed in general under the cover of the housing, connected to a printed circuit containing the safety module. The opening of the cover causes the opening of the switches, which invalid or destroyed the safety module. These switches are more or less numerous following reliability

requested, a large corresponding number with a good reliability.

A disadvantage of these technical is the cost: these switches are expensive components, and their number goes increasing because of

increasingly severe norms of safety.

Another disadvantage is the lack of reliability of these switches, in particular false detections. They arrive often in the

event of shock, particularly when the housing falls. The housing becomes deformed and deviates locally, with the level of one or several switches, pendent a split second. This is particularly penalizing for its owner who cannot then any more use it. In order to limit these false detections, the switches can be equipped with springs intended to absorb the shocks and the vibrations, but this increases the cost of the housing further codes confidential. Another solution consists in filtering low detections of duration to some split seconds by an electronic filter, but this decreases the sensitivity and consequently the reliability of

system anti-intrusion.

A purpose of the invention is to mitigate the abovementioned disadvantages, and particularly to reduce the production costs of the terminals of payment

electronic.

For this purpose, I' invention relates to a device anti-intrusion for protected electronic package (20) which detects any attempt at housing opening. The device comprises a membrane elastomer (50) in which is molded at least a button (51); the button being under pressure when the housing is closed to act on an electronic circuit (60), the button being with

rest when the housing is open.

The invention has for main benefits which it is more reliable than the already known devices anti-intrusions, than it is easy go up, and than it makes it possible to place a large number of buttons, and preferably

in a random way without important overcost compared with the known systems.

▲ top

Other features and benefits of the invention will appear

clearly in the description which will follow and the annexed figures

who represent: - the figure, an example of use of the invention in a self-contain terminal of electronic payment; - the figure Ib, an example of use of the invention in an housing codes confidential connected to a cash register; - figure LLC, an example of use of the invention in protected reader serving as peripheral with a computer; - the figure Id, an example of use of the invention in a distributor of bills; - the figure it, an example of use of the invention in an electronic reader of porte-monnaie; - the figure If, an example of use of the invention in a terminal of communication; - figure 2, an housing codes confidential; - the figures 3a and 3b, the cover and the base of the housing codes confidential represented on figure 2; - the figures 4a and 4b, an example of device anti-intrusion according to the former art;

- the figure 5a, an example of membrane anti elastomer

intrusion according to the invention; - the figure 5b, a cross-section of the membrane represented on the figure 5a;

- the figures 6a and 6b, an example of device anti-intrusion.

according to the invention.

One refers first of all on figures 1 has, 1 B, 1 C, 1 D, 1 E, and 1 F which

possible examples of applications of the invention represent.

The figure L A represents a terminal of electronic payment 1, which is used to carry out payments by bank card particularly in the tradesmen. One still calls this type of terminals of the point-of-sale terminals (TPV) because of their use. This terminal functions in a self-contain way; it is not connected to a cash register. It comprises particularly: a keyboard, being used to the tradesman to seize the post of the transaction, and to the customer to seize his secret code; a bill-poster, to transmit messages to the tradesman or to the customer; a thermal printer for the edition of the tickets; a reader of chip card; a radio connection with a modem; a memory containing for example historical the recorded operations, transactions and a black list. This apparatus must be protected to avoid the risks of fraud, in particular those linked with the reading the given secret ones contained in this terminal. It thus contains a physical device of safety which makes it possible to detect any attempt

of housing opening.

The figure Ib represents an housing codes confidential 2, connected to a cash register. This housing is used to seize the secret code of a bank card, and to check the validity of the entered code. It generally comprises a connection by wire towards the cash register, a cache codes which masque sight of the keyboard of the inquisitive eyes, a bill-poster, a

keyboard, and a reader of chip card. This housing codes confidential is used by the customer only, and does not print a ticket. The entered one of the post of the transaction and the impression of the ticket are carried out on the cash register. A risk of fraud is the interception of the secret code of the bank card. The defrauders modify the housing codes confidential to add a reading device under the keyboard, which transmits the sequence of keys supported by the customer, i.e. the secret code. In order to counter this type of fraud, the housings codes confidential are made safe, and are in measurement to detect any attempt at opening. The figure L C represents a protected reader serving as peripheral with a computer. This reader allows to read chip cards what can be used for example to carry out electronic payments made safe by bank card on Internet, to identify the carrier of a chip card to authorize the access with the given ones contained in the computer, or with reading or writing the given ones on a privative chip card. In I' application of payment made safe on Internet, this reader has at least two benefits: safety and confidentiality. Safety and the confidentiality result owing to the fact that no given concerning the bank card, such that the secret code, the scratch date, the name of the owner of the card, does not circulate into bright on the network. The fraud is possible as from the moment or this reader is modified, this is why it must be made safe and particularly to be

capable to detect any attempt at housing opening.

Figure 1 D represents an automatic distributor of bills 4.

We do not point out here the principle of operation nor its constituting elements. It must be obviously protected counters any attempt at opening

cover, for particularly invalidating the safety module.

The figure represents it a protected reader of chip card 5, being able to be for example an electronic reader of porte-monnaie. This apparatus comprises a physical protection, which particularly makes it possible to detect any attempt at housing opening in order to avoid for example

▲ top

production of false electronic money.

The If figure represents a protected terminal of communication 6.

This terminal can be for example an offering telephone of the services of video in real time as well as an Internet access, comprising preferably a reader of chip card giving access a protected gate. This terminal contains the given confidential ones, such as for example keys of encoding or the given private ones stored in memory. It is equipped with a system which makes it possible to detect any attempt at housing opening, and

who involves the destruction of given confidential.

A common feature of the apparatuses described above, is that they must be in measurement to detect any attempt at opening of their housing or a cover to ensure the integrity or the confidentiality of their contents.

In the description which will follow, we will illustrate an example of

the former art and an application of the invention in an housing codes confidential. One refers on the figure 2 on which an housing is represented codes confidential 20, including/understanding particularly a body of housing 21, a cover of housing 22, a bill-poster 23, a keyboard 24, a reader of chip card 25. The figure 3a represents the cover of the single housing, and the figure 3b represents

the body of housing 21.

One refers now to the figures 4a and 4b to describe an example of realization of device anti-intrusion according to the technical known ones. These figures represent a cross-section of an electronic circuit 40, and a cover of housing 22. The cover 22 belongs to the housing represented on figure 2. Two electronic switches 41 and 42 are placed on the electronic circuit 40. When housing 20 closed like is represented on the figure 4a, its cover 22 rests on switches 41 and 42, which causes to close them. If somebody tries to open the housing, the cover 22 does not rest any more on the switches, which opens them as represented on the figure 4b. Any attempt at intrusion is thus detected by the circuit connected to each switch, which causes to invalidate the module

of safety.

A disadvantage of this technical is its cost: the switches are expensive and complex components to go up, and their number goes

increasing because of increasingly severe norms of safety.

Another disadvantage is the lack of reliability of these switches, in particular false detections. They arrive often in the event of shock, particularly when the housing falls. The housing becomes deformed and deviates locally, with the level of one or several switches, pendent a split second. This is particularly penalizing for its owner who cannot then any more use it. In order to limit these false detections, the switches can be equipped with springs intended to absorb the shocks and the vibrations, but this increases the cost of the housing further codes confidential. Another solution consists in filtering detections of low durations to some split seconds by an electronic filter, but this decreases the sensitivity and consequently the reliability of

system anti-intrusion.

One refers now to the figures 5a and 5b which represents an example of realization of membrane elastomer anti-intrusion according to the invention. This membrane 50, out of elastomeric material such as silicone, belongs to the keyboard 24 of the housing codes confidential 20 represented on figure 2. It contains the buttons of the keys of the keyboard 24, such as for example buttons 54, 55, 56. It contains also three buttons 51, 52, 53, which are approximately for example less high than the buttons of key of keyboard. The molded buttons in the membrane are covered with a conductive substrate as represented on the cross-section appears 5b: for example it

button 52 includes/understands an extended pin 57 by a carbon 58 portion.

One refers also to the figures 6a and 6b which represents this cross-section membrane with other elements. The membrane is placed under the cover 22 of housing 20 represented on figures 2 and 3a. An electronic circuit 60, particularly making it possible to detect the keys of the keyboard supported, is placed under the membrane. When the housing is closed like

represented on the figure 6a, the cover 22 rests on buttons 51, 52, 53.

▲ top

These buttons are depressed under the pressure exerted by the cover 22 compared to their home position. The conductive portion of the buttons is consequently in contact with the electronic circuit 60. These points of conductive contacts make it possible to connect between them conductive tracks of circuit 60. Thus, buttons 51, 52 and 53 establish electrical connections in circuit 60 as long as the housing is closed. When the housing open like is represented on the figure 5b, the cover 22 does not rest any more on buttons 51, 52, 53. These buttons are put then in their home position and are not any more in contact with the electronic circuit 60. They function with the manner of switches which make it possible to detect any attempt at opening of

housing.

A benefit of the invention compared to the former art is the economy on the components. When buttons are added, the price of the membrane is not changed because it is enough to modify the mould of manufacture and to add the conductive same substrate that on the keys of keyboards. That is to be compared for example with the switches whose addition increases the cost of the device anti-intrusion at least price of the switches. One saves thanks to the invention the induced cost by the addition of switches. One can thus make the device anti-intrusion more reliable by adding buttons, without

for increasing its cost as much.

Another benefit of the invention is the reliability of the anti device

intrusion. Indeed, the properties of elasticity of the membrane avoid false detection induced particularly by shocks. The membrane thus preferably replaces the mechanical or electronic filters which

could decrease the sensitivity of the device anti-intrusion.

Another benefit of the invention is its facility of mounting. The membrane is simply laid to be placement. It does not require a welding or of other mechanical intervention to bind it to the other present components in the housing. Consequently, times of mounting are reduced compared to technical known using

switches, which contributes to an additional reduction of cost.

According to an advantageous alternative, the buttons being used to detect the housing opening can be distributed by chance on the surface of the membrane. Thus, the defrauders will not be able to locate the site of the devices anti-intrusion on an housing to thwart the system of safety of another of the same housing model. It is enough for that to envisage several moulds of manufacture of membrane with different distributions of these buttons. The electronic circuits will be them also manufactured with conductive tracks whose positions depend on those of the buttons. Compared to the devices anti-intrusion containing electronic switches, this present solution the benefit to be feasible readily on a chain

of mounting, and thus at lesser cost.

Of course, the present invention is not limited to the form of

realization described herebefore as example. It extends to other alternatives.

One will understand as well as the membrane was described with three buttons being used to detect the housing opening, but that the invention

applique also with any membrane including/understanding another number of buttons.

This number can be more or less important according to for example the level of

requested safety or size of the membrane elastomer.

Moreover, the membrane on which are placed the buttons is not necessarily a membrane of keyboard. In particular, this membrane can contain only buttons being used to detect the housing opening and any other type of button. It can for example contain one button, or a very large number of buttons. Such an alternative of realization particularly makes it possible to preferably replace a device containing a very large number of electronic switches

being used to detect the housing opening.

In the description which precedes, the cover rests on the membrane,

but the device anti-intrusion according to the invention functions just as easily if another mechanical part that the cover
top rests on the membrane. The membrane can for example be placed under another component contained in the housing, such as for example a second electronic circuit. The first electronic circuit placed under the membrane contains the means of treatments on which act the abovementioned buttons; the second electronic circuit placed on the membrane puts in pressure the buttons when it

housing is closed.

The invention applique of course with any type of protected electronic package. Of general manner, it applique with the protected housings which one seeks to guarantee the physical integrity by a mean of

detection of opening.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 806 507**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **00 03465**

(51) Int Cl[7] : **G 08 B 13/00**, G 07 F 7/08, G 06 K 19/07

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 17.03.00.

(30) **Priorité** :

(43) **Date de mise à la disposition du public de la demande** : 21.09.01 Bulletin 01/38.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *DASSAULT AUTOMATISMES ET TELECOMMUNICATIONS Société anonyme* — FR.

(72) **Inventeur(s)** : MOREE PASCAL.

(73) **Titulaire(s)** :

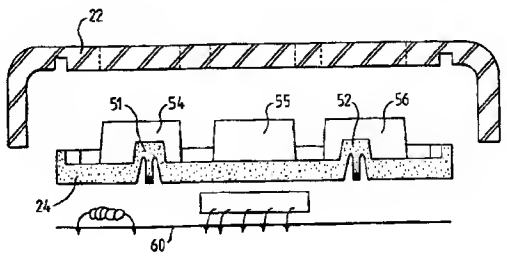
(74) **Mandataire(s)** : THALES "INTELLECTUAL PROPERTY".

(54) MEMBRANE ELASTOMERE ANTI-INTRUSION POUR BOITIERS ELECTRONIQUES SECURISES.

(57) La présente invention se rapporte à une membrane élastomère anti-intrusion pour boîtiers électroniques sécurisés.

Dans cette membrane élastomère (50) est moulé au moins un bouton (51); le bouton étant sous pression lorsque le boîtier est fermé pour agir sur un circuit électronique (60), le bouton étant au repos lorsque le boîtier est ouvert.

Elle s'applique aux boîtiers sécurisés, tels que notamment les boîtiers codes confidentiels, dont on cherche à garantir l'intégrité physique par un moyen de détection d'ouverture.



FR 2 806 507 - A1

La présente invention se rapporte à une membrane élastomère anti-intrusion pour boîtiers électroniques sécurisés. Elle s'applique aux boîtiers sécurisés, tel que notamment les boîtiers codes confidentiels, dont on cherche à garantir l'intégrité physique par un moyen de détection d'ouverture.

Les boîtiers électroniques sécurisés sont utilisés dans de nombreuses applications et permettent notamment de lire des cartes à puce telles que par exemple des cartes bancaires, des porte-monnaie électroniques, des cartes multiservices (téléphonique, bancaire, porte-monnaie électronique, santé...) ou encore des cartes de paiement privatives. Afin d'éviter les fraudes, ils sont équipés de systèmes protections, tels que des dispositifs anti-intrusion, qui garantissent leur intégrité physique.

On peut citer l'exemple des terminaux de paiement électronique (TPE), notamment par carte bancaire. Ces terminaux électroniques sont la cible d'escrocs qui tentent par tous les moyens de les ouvrir et les modifier pour une utilisation frauduleuse. En réaction, les organismes de carte bancaire, telle que Visa International, imposent des normes de sécurité contraignantes pour homologuer ces terminaux de paiement. Selon l'une de ces normes, les terminaux doivent être en mesure de détecter toute tentative d'ouverture de leur boîtier. La détection de l'ouverture entraîne notamment la mise hors service du module de sécurité, lequel contient par exemple un ensemble d'algorithmes cryptographiques et de codes secrets servant à valider la carte à puce ou carte à piste magnétique et à assurer l'intégrité des informations de paiement (compteurs d'unités ou transactions).

Les terminaux de paiement électronique par carte bancaire comportent parfois des boîtiers codes confidentiels, encore appelés Pinpad dans la littérature anglo-saxonne. Ces boîtiers servent à lire une carte bancaire, entrer son code secret, et vérifier la validité du code entré. Ils comportent généralement un clavier numérique, un écran à cristaux liquides, un lecteur de carte à puce, éventuellement un cache code, et une connexion par fil à un terminal point de vente. Dans cet exemple, le terminal de paiement électronique est l'ensemble constitué du boîtier code confidentiel et du terminal point de vente.

Dans les techniques actuelles, les terminaux de paiement électronique sont équipés d'interrupteurs qui détectent l'ouverture. Ces interrupteurs sont placés en général sous le capot du boîtier, connectés à un circuit imprimé contenant le module de sécurité. L'ouverture du capot provoque l'ouverture des interrupteurs, ce qui invalide ou détruit le module de sécurité. Ces interrupteurs sont plus ou moins nombreux suivant la fiabilité requise, un grand nombre correspondant à une meilleure fiabilité.

Un inconvénient de ces techniques est le coût : ces interrupteurs sont des composants onéreux, et leur nombre va croissant à cause de normes de sécurité de plus en plus sévères.

Un autre inconvénient est le manque de fiabilité de ces interrupteurs, en particulier les fausses détections. Elles arrivent souvent en cas de choc, notamment lorsque le boîtier tombe. Le boîtier se déforme et s'écarte localement, au niveau d'un ou plusieurs interrupteurs, pendant une fraction de seconde. Ceci est particulièrement pénalisant pour son propriétaire qui ne peut alors plus l'utiliser. Afin de limiter ces fausses détections, les interrupteurs peuvent être équipés de ressorts destinés à absorber les chocs et les vibrations, mais ceci augmente encore le coût du boîtier code confidentiel. Une autre solution consiste à filtrer les détections de durée inférieures à quelques fractions de secondes par un filtre électronique, mais ceci diminue la sensibilité et par conséquent la fiabilité du système anti-intrusion.

Un but de l'invention est de pallier les inconvénients précités, et notamment de réduire les coûts de production des terminaux de paiement électronique.

A cet effet, l'invention concerne un dispositif anti-intrusion pour boîtier électronique sécurisé (20) qui détecte toute tentative d'ouverture du boîtier. Le dispositif comporte une membrane élastomère (50) dans laquelle est moulé au moins un bouton (51) ; le bouton étant sous pression lorsque le boîtier est fermé pour agir sur un circuit électronique (60), le bouton étant au repos lorsque le boîtier est ouvert.

L'invention a pour principaux avantages qu'elle est plus fiable que les dispositifs anti-intrusions déjà connus, qu'elle est facile à monter, et qu'elle permet de placer un grand nombre de boutons, et avantageusement de façon aléatoire sans surcoût important comparé aux systèmes connus.

D'autres caractéristiques et avantages de l'invention apparaîtront plus clairement dans la description qui va suivre et dans les figures annexées qui représentent :

- la figure 1a, un exemple d'utilisation de l'invention dans un terminal de paiement électronique autonome ;
- la figure 1b, un exemple d'utilisation de l'invention dans un boîtier code confidentiel relié à une caisse enregistreuse ;
- la figure 1c, un exemple d'utilisation de l'invention dans lecteur sécurisé servant de périphérique à un ordinateur ;
- la figure 1d, un exemple d'utilisation de l'invention dans un distributeur de billets ;
- la figure 1e, un exemple d'utilisation de l'invention dans un lecteur de porte-monnaie électronique ;
- la figure 1f, un exemple d'utilisation de l'invention dans un terminal de communication ;
- la figure 2, un boîtier code confidentiel ;
- les figures 3a et 3b, le capot et le socle du boîtier code confidentiel représenté sur la figure 2 ;
- les figures 4a et 4b, un exemple de dispositif anti-intrusion selon l'art antérieur ;
- la figure 5a, un exemple de membrane élastomère anti-intrusion selon l'invention ;
- la figure 5b, une vue en coupe de la membrane représentée sur la figure 5a ;
- les figures 6a et 6b, un exemple de dispositif anti-intrusion. selon l'invention.

On se réfère tout d'abord aux figures 1a, 1b, 1c, 1d, 1e, et 1f qui représentent des exemples d'applications possibles de l'invention.

La figure 1a représente un terminal de paiement électronique 1, qui sert à effectuer des paiements par carte bancaire notamment chez les commerçants. On appelle encore ce type de terminaux des terminaux point de vente (TPV) en raison de leur usage. Ce terminal fonctionne de façon autonome ; il n'est pas relié à une caisse enregistreuse. Il comporte notamment : un clavier, servant au commerçant pour saisir le montant de la

transaction, et au client pour saisir son code secret ; un afficheur, pour transmettre des messages au commerçant ou au client ; une imprimante thermique pour l'édition des tickets ; un lecteur de carte à puce ; une liaison radio avec un modem ; une mémoire contenant par exemple un historique des opérations, les transactions enregistrées et une liste noire. Cet appareil doit être sécurisé pour éviter les risques de fraude, en particulier ceux liés à la lecture de données secrètes contenues dans ce terminal. Il contient donc un dispositif physique de sécurité qui permet de détecter toute tentative d'ouverture du boîtier.

La figure 1b représente un boîtier code confidentiel 2, relié à une caisse enregistreuse. Ce boîtier sert à saisir le code secret d'une carte bancaire, et à vérifier la validité du code entré. Il comporte généralement une liaison par fil vers la caisse enregistreuse, un cache code qui masque la vue du clavier des regards indiscrets, un afficheur, un clavier, et un lecteur de carte à puce. Ce boîtier code confidentiel est utilisé par le client uniquement, et n'imprime pas de ticket. La saisie du montant de la transaction et l'impression du ticket s'effectuent sur la caisse enregistreuse. Un risque de fraude est l'interception du code secret de la carte bancaire. Les fraudeurs modifient le boîtier code confidentiel pour ajouter un dispositif de lecture sous le clavier, qui transmet la séquence de touches appuyées par le client, c'est à dire le code secret. Afin de contrer ce type de fraude, les boîtiers code confidentiel sont sécurisés, et sont en mesure de détecter toute tentative d'ouverture.

La figure 1c représente un lecteur sécurisé servant de périphérique à un ordinateur. Ce lecteur permet de lire des cartes à puce ce qui peut servir par exemple à effectuer des paiements électroniques sécurisés par carte bancaire sur Internet, à identifier le porteur d'une carte à puce pour autoriser l'accès à des données contenues dans l'ordinateur, ou encore à lire ou écrire des données sur une carte à puce privative. Dans l'application de paiement sécurisé sur Internet, ce lecteur a au moins deux avantages : la sécurité et la confidentialité. La sécurité et la confidentialité résultent du fait qu'aucune donnée concernant la carte bancaire, tel que le code secret, la date d'expiration, le nom du propriétaire de la carte, ne circule en clair sur le réseau. La fraude est possible à partir du moment ou ce

lecteur est modifié, c'est pourquoi il doit être sécurisé et notamment être capable de détecter toute tentative d'ouverture du boîtier.

La figure 1d représente un distributeur automatique de billets 4. Nous ne rappelons pas ici le principe de fonctionnement ni ses éléments constitutifs. Il doit être évidemment protégé contre toute tentative d'ouverture du capot, pour notamment invalider le module de sécurité.

La figure 1e représente un lecteur sécurisé de carte à puce 5, pouvant être par exemple un lecteur de porte-monnaie électronique. Cet appareil comporte une protection physique, qui permet notamment de détecter toute tentative d'ouverture du boîtier afin d'éviter par exemple la production de fausse monnaie électronique.

La figure 1f représente un terminal de communication sécurisé 6. Ce terminal peut être par exemple un téléphone offrant des services de vidéo en temps réel ainsi qu'un accès à Internet, comportant avantageusement un lecteur de carte à puce permettant d'accéder à un portail sécurisé. Ce terminal contient des données confidentielles, telles que par exemple des clefs de cryptage ou des données privées stockées en mémoire. Il est équipé d'un système qui permet de détecter toute tentative d'ouverture du boîtier, et qui entraîne la destruction des données confidentielles.

Une caractéristique commune des appareils décrits ci-dessus, est qu'ils doivent être en mesure de détecter toute tentative d'ouverture de leur boîtier ou d'un capot pour assurer l'intégrité ou la confidentialité de leur contenu.

Dans la description qui va suivre, nous illustrerons un exemple de l'art antérieur et une application de l'invention dans un boîtier code confidentiel. On se réfère à la figure 2 sur laquelle est représenté un boîtier code confidentiel 20, comprenant notamment un corps de boîtier 21, un capot de boîtier 22, un afficheur 23, un clavier 24, un lecteur de carte à puce 25. La figure 3a représente le capot du boîtier seul, et la figure 3b représente le corps du boîtier 21.

On se réfère maintenant aux figures 4a et 4b pour décrire un exemple de réalisation de dispositif anti-intrusion selon les techniques connues. Ces figures représentent une vue en coupe d'un circuit électronique 40, et d'un capot de boîtier 22. Le capot 22 appartient au boîtier

20 représenté sur la figure 2. Deux interrupteurs électroniques 41 et 42 sont placés sur le circuit électronique 40. Lorsque le boîtier 20 est fermé comme représenté sur la figure 4a, son capot 22 repose sur les interrupteurs 41 et 42, ce qui a pour effet de les fermer. Si quelqu'un tente d'ouvrir le boîtier, le capot 22 ne repose plus sur les interrupteurs, ce qui les ouvre comme représenté sur la figure 4b. Toute tentative d'intrusion est ainsi détectée par le circuit relié à chaque interrupteur, ce qui a pour effet d'invalider le module de sécurité.

Un inconvénient de cette technique est son coût : les interrupteurs sont des composants onéreux et complexes à monter, et leur nombre va croissant à cause de normes de sécurité de plus en plus sévères.

Un autre inconvénient est le manque de fiabilité de ces interrupteurs, en particulier les fausses détections. Elles arrivent souvent en cas de choc, notamment lorsque le boîtier tombe. Le boîtier se déforme et s'écarte localement, au niveau d'un ou plusieurs interrupteurs, pendant une fraction de seconde. Ceci est particulièrement pénalisant pour son propriétaire qui ne peut alors plus l'utiliser. Afin de limiter ces fausses détections, les interrupteurs peuvent être équipés de ressorts destinés à absorber les chocs et les vibrations, mais ceci augmente encore le coût du boîtier code confidentiel. Une autre solution consiste à filtrer les détections de durées inférieures à quelques fractions de secondes par un filtre électronique, mais ceci diminue la sensibilité et par conséquent la fiabilité du système anti-intrusion.

On se réfère maintenant aux figures 5a et 5b qui représentent un exemple de réalisation de membrane élastomère anti-intrusion selon l'invention. Cette membrane 50, en matière élastomère telle que le silicone, appartient au clavier 24 du boîtier code confidentiel 20 représenté sur la figure 2. Elle contient les boutons des touches du clavier 24, tels que par exemple les boutons 54, 55, 56. Elle contient aussi trois boutons 51, 52, 53, qui sont environ par exemple moins hauts que les boutons de touche de clavier. Les boutons moulés dans la membrane sont recouverts d'un substrat conducteur tel que représenté sur la vue en coupe figure 5b : par exemple le bouton 52 comprend un ergot 57 prolongé par une partie en carbone 58.

On se réfère aussi aux figures 6a et 6b qui représentent cette membrane vue en coupe avec d'autres éléments. La membrane est placée

sous le capot 22 du boîtier 20 représenté sur les figures 2 et 3a. Un circuit électronique 60, permettant notamment de détecter les touches du clavier appuyées, est placé sous la membrane. Lorsque le boîtier est fermé comme représenté sur la figure 6a, le capot 22 repose sur les boutons 51, 52, 53. Ces boutons sont enfoncés sous la pression exercée par le capot 22 par rapport à leur position de repos. La partie conductrice des boutons est par conséquent en contact avec le circuit électronique 60. Ces points de contacts conducteurs permettent de relier entre elles des pistes conductrices du circuit 60. Ainsi, les boutons 51, 52 et 53 établissent des liaisons électriques dans le circuit 60 tant que le boîtier est fermé. Lorsque le boîtier est ouvert comme représenté sur la figure 5b, le capot 22 ne repose plus sur les boutons 51, 52, 53. Ces boutons se mettent alors dans leur position de repos et ne sont plus en contact avec le circuit électronique 60. Ils fonctionnent à la manière d'interrupteurs qui permettent de détecter toute tentative d'ouverture du boîtier.

Un avantage de l'invention par rapport à l'art antérieur est l'économie sur les composants. Lorsqu'on ajoute des boutons, on ne change pas le prix de la membrane car il suffit de modifier le moule de fabrication et d'ajouter le même substrat conducteur que sur les touches de claviers. Cela est à comparer par exemple aux interrupteurs dont l'ajout augmente le coût du dispositif anti-intrusion au moins du prix des interrupteurs. On économise grâce à l'invention le coût induit par l'ajout d'interrupteurs. On peut donc rendre le dispositif anti-intrusion plus fiable en ajoutant des boutons, sans pour autant augmenter son coût.

Un autre avantage de l'invention est la fiabilité du dispositif anti-intrusion. En effet, les propriétés d'élasticité de la membrane évitent les fausses détection induites notamment par des chocs. La membrane remplace ainsi avantageusement les filtres mécaniques ou électroniques qui pouvaient diminuer la sensibilité du dispositif anti-intrusion.

Un autre avantage de l'invention est sa facilité de montage. La membrane est simplement posée pour être mise en place. Elle ne requiert pas de soudure ou d'autre intervention mécanique pour la lier aux autres composants présents dans le boîtier. En conséquence, les temps de montage sont réduits par rapport aux techniques connues utilisant des interrupteurs, ce qui contribue à une réduction de coût additionnelle.

Selon une variante avantageuse, les boutons servant à détecter l'ouverture du boîtier peuvent être répartis aléatoirement sur la surface de la membrane. Ainsi, les fraudeurs ne pourront pas localiser l'emplacement des dispositifs anti-intrusion sur un boîtier pour déjouer le système de sécurité d'un autre boîtier de même modèle. Il suffit pour cela de prévoir plusieurs moules de fabrication de membrane avec des répartitions différentes de ces boutons. Les circuits électroniques seront eux aussi fabriqués avec des pistes conductrices dont les positions dépendent de celles des boutons. Par rapport aux dispositifs anti-intrusion à base d'interrupteurs électroniques, cette solution présente l'avantage d'être réalisable facilement sur une chaîne de montage, et donc à moindre coût.

Bien entendu, la présente invention ne se limite pas à la forme de réalisation décrite ci-avant à titre d'exemple. Elle s'étend à d'autres variantes.

On comprendra ainsi que la membrane a été décrite avec trois boutons servant à détecter l'ouverture du boîtier, mais que l'invention s'applique aussi à toute membrane comprenant un autre nombre de boutons. Ce nombre peut être plus ou moins important selon par exemple le niveau de sécurité requis ou encore la taille de la membrane élastomère.

En outre, la membrane sur laquelle sont placés les boutons n'est pas nécessairement une membrane de clavier. En particulier, cette membrane peut ne contenir que des boutons servant à détecter l'ouverture du boîtier et aucun autre type de bouton. Elle peut par exemple ne contenir qu'un seul bouton, ou encore un très grand nombre de boutons. Une telle variante de réalisation permet notamment de remplacer avantageusement un dispositif contenant un très grand nombre d'interrupteurs électroniques servant à détecter l'ouverture du boîtier.

Dans la description qui précède, le capot repose sur la membrane, mais le dispositif anti-intrusion selon l'invention fonctionne tout aussi bien si une autre pièce mécanique que le capot repose sur la membrane. La membrane peut par exemple être placée sous un autre composant contenu dans le boîtier, tel que par exemple un deuxième circuit électronique. Le premier circuit électronique placé sous la membrane contient les moyens de traitements sur lesquels agissent les boutons précités ; le second circuit électronique placé sur la membrane met en pression les boutons lorsque le boîtier est fermé.

L'invention s'applique bien entendu à tout type de boîtier électronique sécurisé. De manière générale, elle s'applique aux boîtiers sécurisés dont on cherche à garantir l'intégrité physique par un moyen de détection d'ouverture.

REVENDICATIONS

1. Dispositif anti-intrusion pour boîtier électronique sécurisé (20) qui détecte toute tentative d'ouverture du boîtier, caractérisé en ce que ledit dispositif comporte une membrane élastomère (50) dans laquelle est moulé au moins un bouton (51) ; le bouton étant sous pression lorsque le boîtier est fermé pour agir sur un circuit électronique (60), le bouton étant au repos lorsque le boîtier est ouvert.

2. Dispositif anti-intrusion selon la revendication précédente, caractérisé en ce que l'action entre le bouton et le circuit électronique se fait par un contact électrique entre une partie conductrice appartenant au bouton et des pistes conductrices appartenant au circuit.

3. Dispositif anti-intrusion selon l'une des revendications précédentes, caractérisé en ce que la membrane comporte en outre des boutons de touche de clavier.

4. Dispositif anti-intrusion selon l'une des revendications précédentes, caractérisé en ce que la membrane élastomère est placée en contact avec au moins un élément mécanique agissant sur au moins un bouton de détection d'ouverture lorsque le boîtier est fermé, et n'agissant plus dessus lorsque le boîtier est ouvert.

5. Dispositif anti-intrusion selon l'une des revendications précédentes, caractérisé en ce que la membrane élastomère est placée entre un capot (22) et un circuit électronique (60).

6. Dispositif anti-intrusion selon l'une des revendications précédentes, caractérisé en ce que le boîtier électronique sécurisé est un boîtier code confidentiel.

7. Dispositif anti-intrusion selon l'une des revendications 1 à 5, caractérisé en ce que le boîtier électronique sécurisé est un terminal de paiement électronique.

8. Dispositif anti-intrusion selon l'une des revendications 1 à 5, caractérisé en ce que le boîtier électronique sécurisé est lecteur de porte-monnaie électronique.

9. Dispositif anti-intrusion selon l'une des revendications 1 à 5, caractérisé en ce que le boîtier électronique sécurisé est un terminal de communication.

10. Dispositif anti-intrusion selon l'une des revendications 1 à 5, caractérisé en ce que le boîtier électronique sécurisé est un terminal de communication comportant un lecteur de carte à puce.

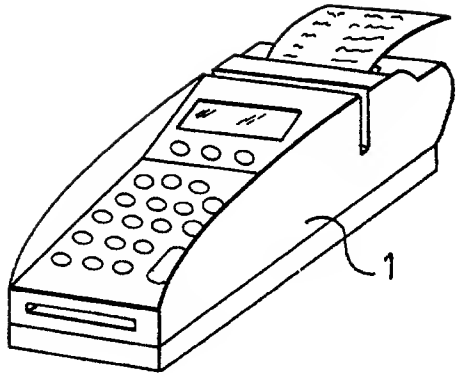


FIG.1a

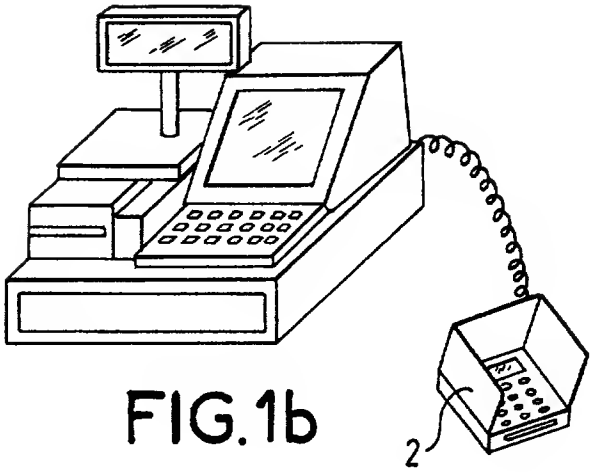


FIG.1b

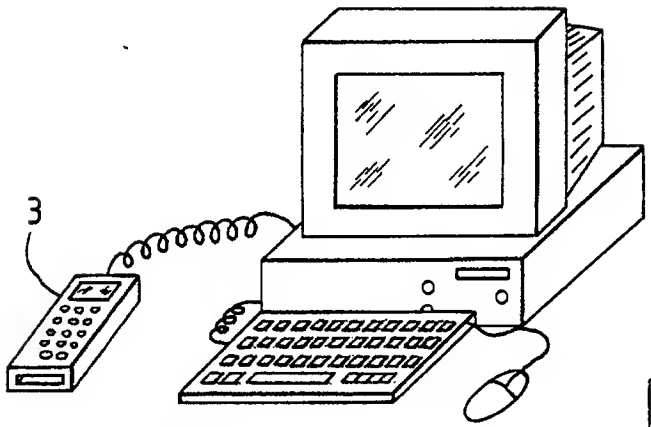


FIG.1c

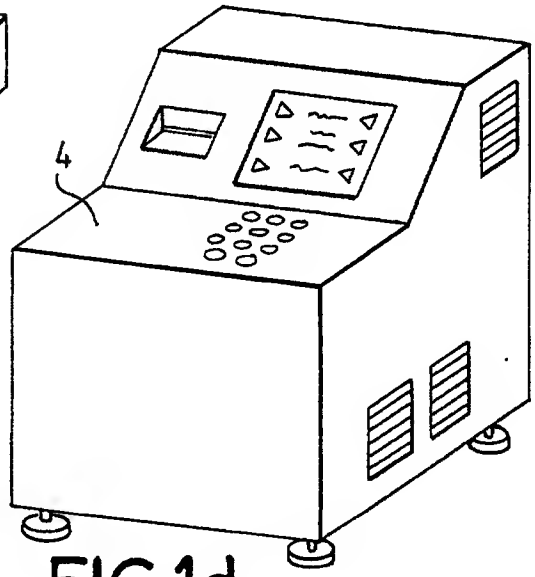


FIG.1d

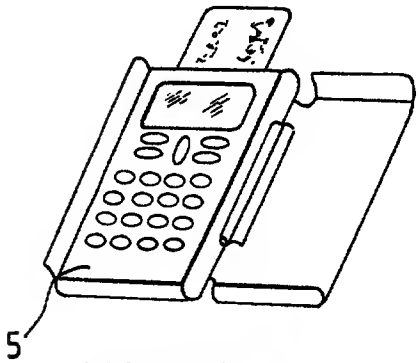


FIG.1e

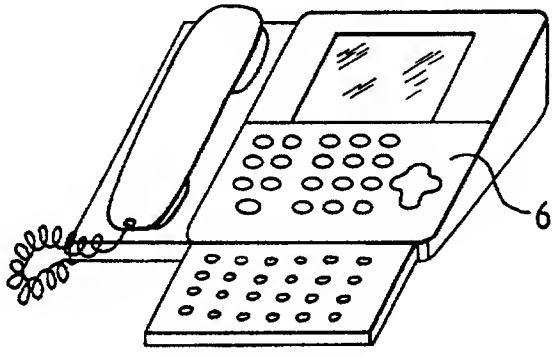


FIG.1f

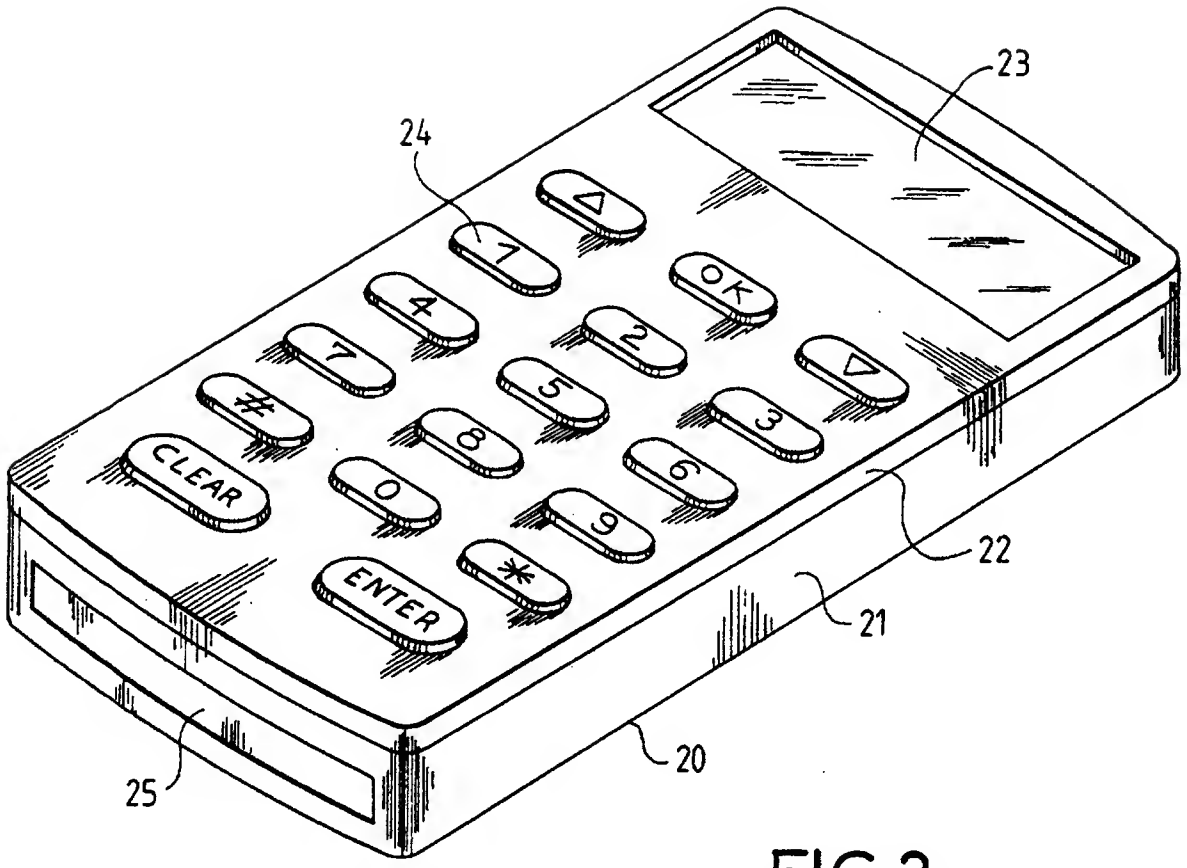
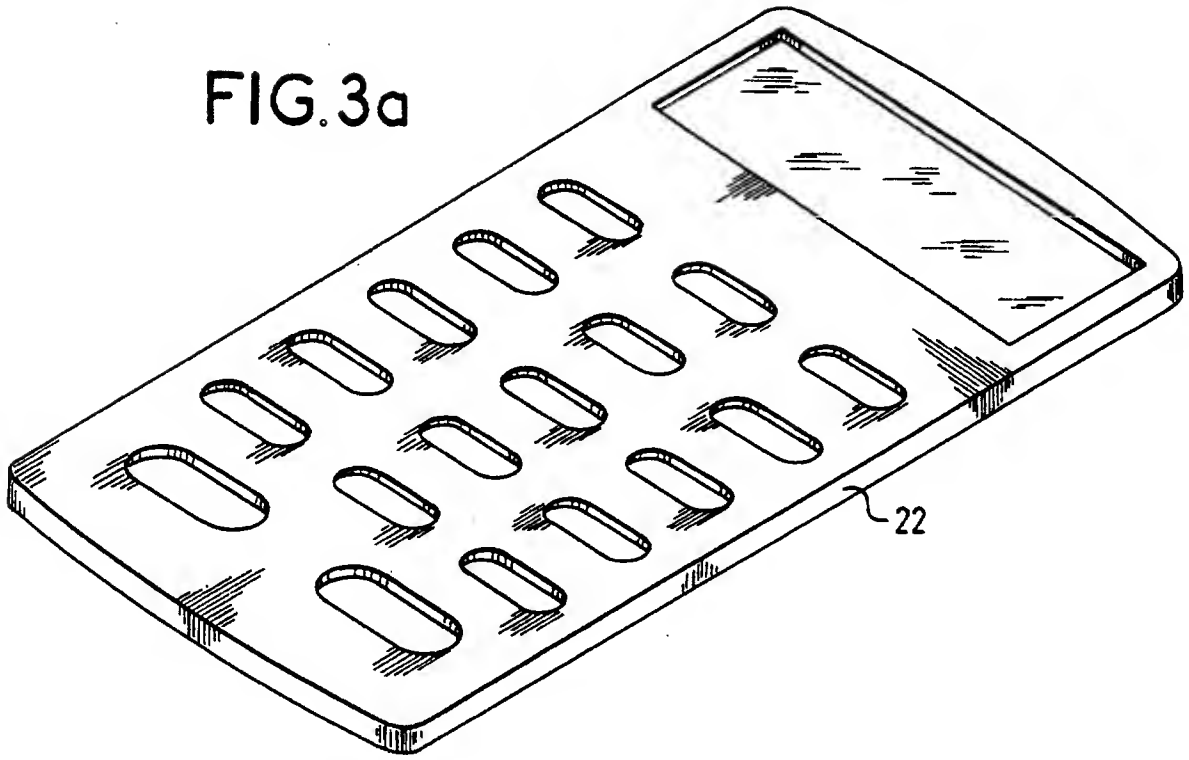


FIG.2

FIG.3a



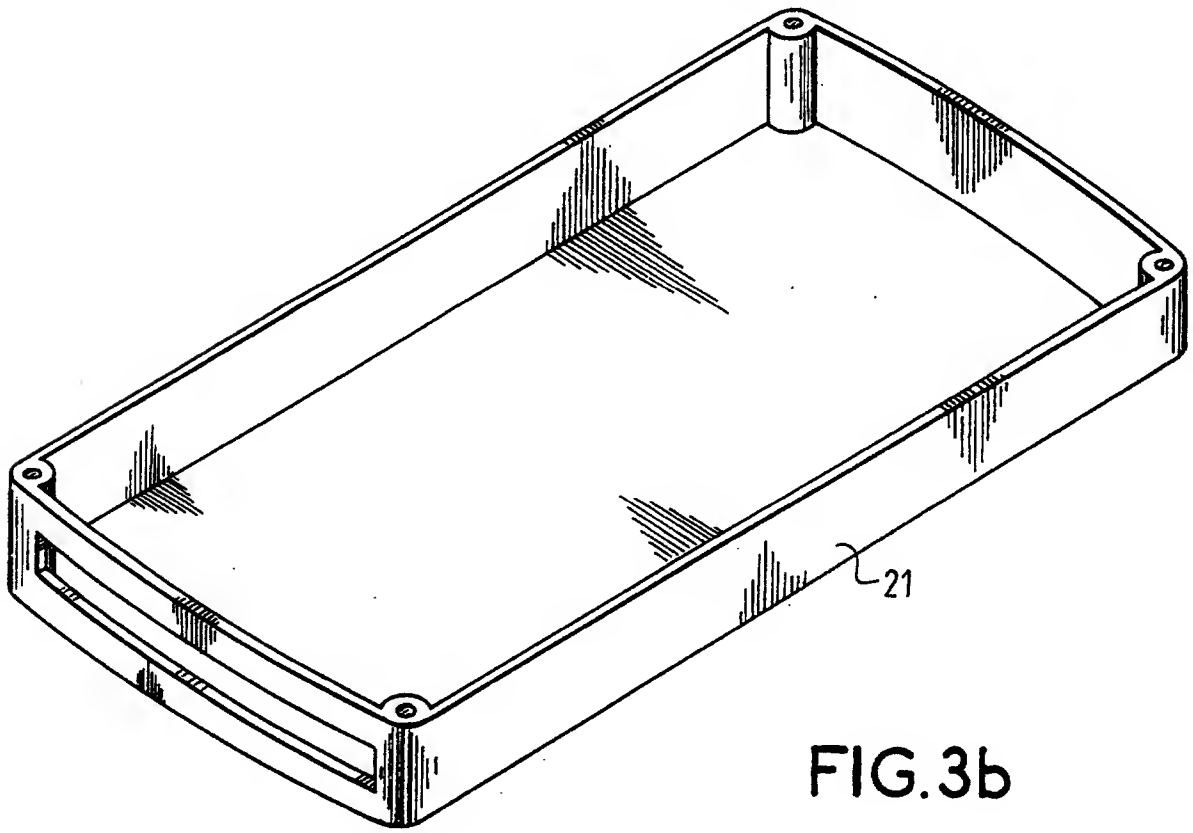


FIG.3b

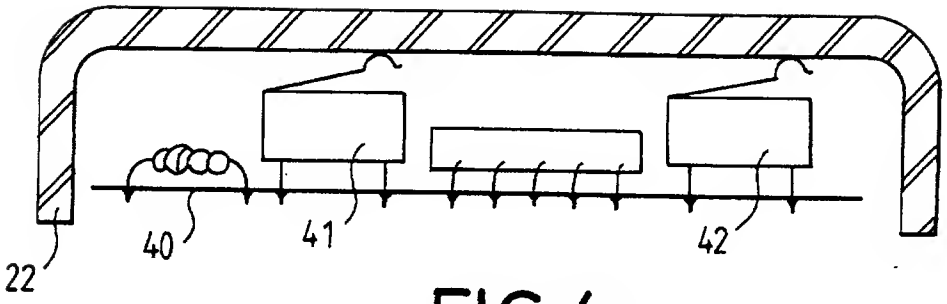


FIG.4a

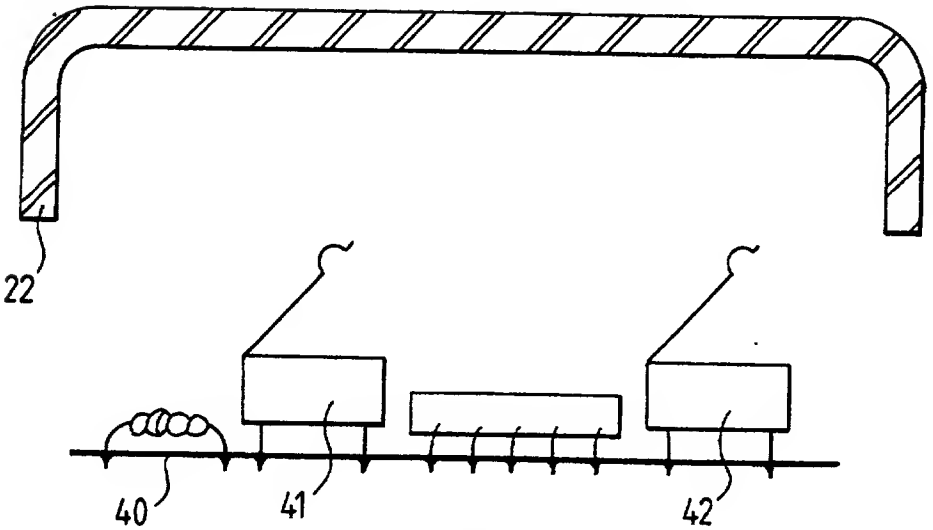


FIG.4b

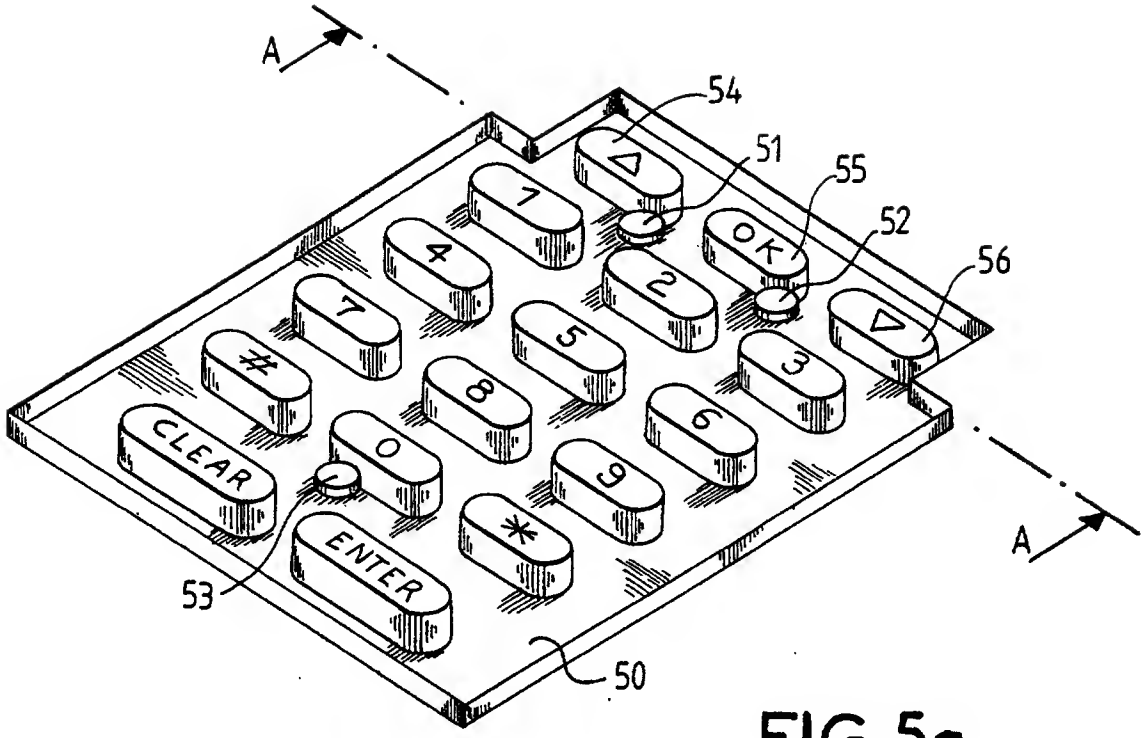
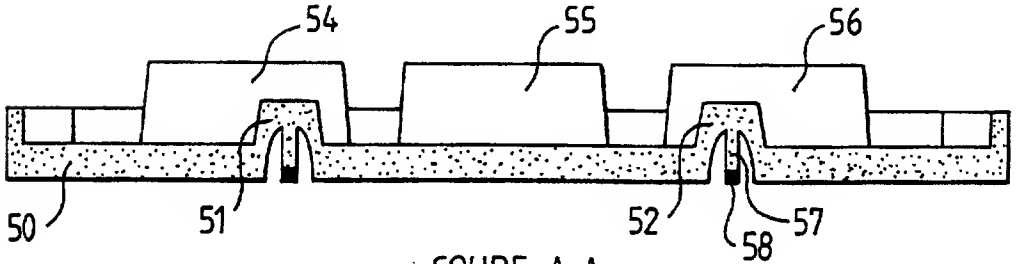


FIG. 5a



COUPE A-A

FIG. 5b

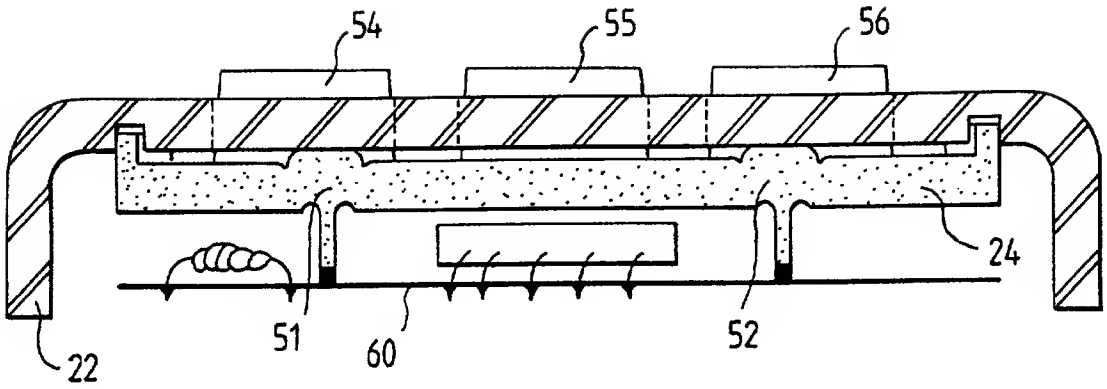


FIG. 6a

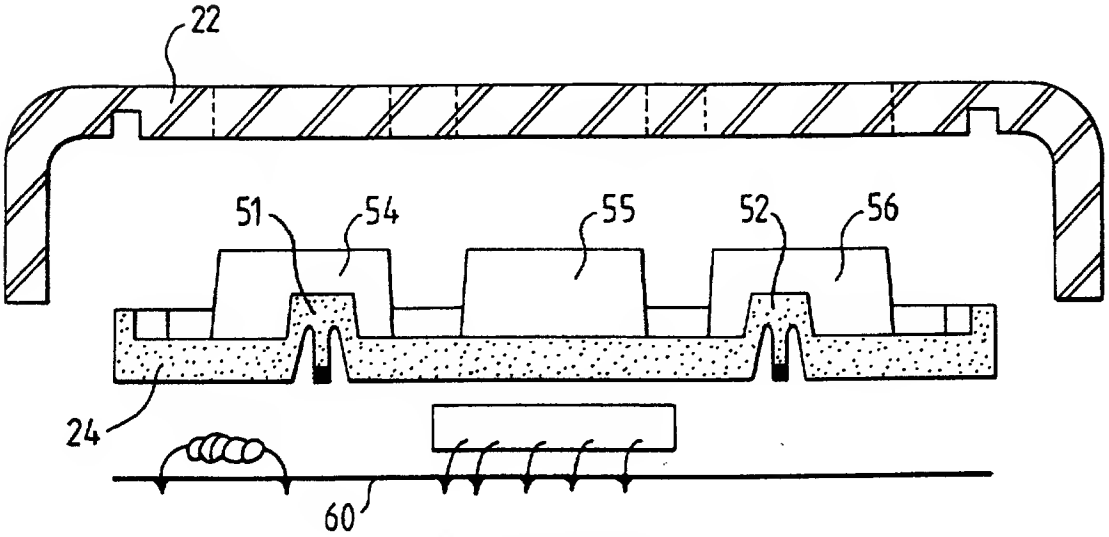


FIG. 6b

RÉPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

2806507

N° d'enregistrement national

FA 585305
FR 0003465

RAPPORT DE RECHERCHE PRÉLIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

DOCUMENTS CONSIDÉRÉS COMME PERTINENTS		Revendication(s) concernée(s)	Classement attribué à l'Invention par l'INPI
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes		
X	DE 43 12 905 A (KRONE AG) 20 octobre 1994 (1994-10-20) * colonne 2, ligne 40 - ligne 60 * * colonne 3, ligne 16 - ligne 31 * ---	1-10	G08B13/00 G07F7/08 G06K19/07
X	DE 91 05 960 U (SIEMENS NIXDORF INF. SYST.) 11 juin 1992 (1992-06-11) * page 5, ligne 5 * ---	1,2,4-10	
A	DE 197 05 518 A (SIEMENS AG) 27 août 1998 (1998-08-27) * le document en entier * -----	1-10	
			DOMAINES TECHNIQUES RECHERCHÉS (Int.Cl.7)
			G08B G06F G07F G06K

Date d'achèvement de la recherche: 7 décembre 2000

Examinateur: De la Cruz Valera, D

CATÉGORIE DES DOCUMENTS CITÉS

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : arrière-plan technologique
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 12.99 (P04C14)